REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE:	3. REPORT TYPE AND DATES COVERED Final Report 18-Aug-2003 - 17-Dec-2005

4. TITLE AND SUBTITLE
Advanced Quantum Communication Protocols

5. FUNDING NUMBERS
DAAD190310282

6. AUTHORS
Paul Kwiat

8. PERFORMING ORGANIZATION REPORT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Illinois - Urbana
Grants and Contracts Office
109 Coble Hall
Champaign, IL 61820 -6242

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
45564-PH-QC.1

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The abstract is below since many authors do not follow the 200 word limit

14. SUBJECT TERMS
quantum cryptography, entanglement, random number generator, remote state preparation, quantum dense coding

15. NUMBER OF PAGES
Unknown due to possible attachments

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Report Title

Advanced Quantum Communication Protocols

ABSTRACT

We have realized the first demonstration of "relativistic" quantum cryptography, using both faint laser pulses and entangled photons. By incorporating an optical delay cavity, Bob is able to measure every photon from Alice in the correct basis, leading to enhanced key rates, as well as some security advantages. We have also implemented our proposal for a high-speed quantum random number generator, in which the arrival time of a detected photon is used to generate ~8 random bits per photon. Our system produced cryptographically secure bits at over 4 Mbits/s, with a clear path toward even higher rates. In addition, we solved a number of technical problems to produce 99%-fidelity polarization-entangled pairs from a diode-laser pumped source. Extending our previous implementation of remote state preparation, we have incorporated hyperentanglement to successfully remotely prepare entangled states. Finally, we studied the use of hyperentangled photons as a resource for improved quantum dense coding. Although our experimental verification is still in progress, we identified the theoretically optimal configuration, and compared hyperentangled and multi-pair encoding.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

1. "Generation of hyper-entangled photon pairs", J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. 95, 260501 (2005).
2. "Phase-compensated ultra-bright source of entangled photons", J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, Opt. Expr. 13, 8951 (2005).
3. "Optical Implementation of Quantum Orienteering", E. R. Jeffrey, J. B. Altepeter, M. Colci, and P. G. Kwiat, Phys. Rev. Lett. 96, 150503. (2006).

Number of Papers published in peer-reviewed journals: 3.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

1. "Quantum Orienteering", P. G. Kwiat, E. R. Jeffrey, and J. B. Altepeter, SPIE 2005, San Diego, CA, Aug. 1 – 4, 2005.
2. "The Entanglement Revolution", P. G. Kwiat, Entry in Amazing Light: Young Scholars Competition, as part of Visions for Discovery symposium in honor of Charles Townes' 90th Birthday, U.C., Berkeley, Oct. 5-7, 2005.
3. "Hyperentanglement: When One Degree of Freedom Isn't Enough", 36th Winter Colloquium on the Physics of Quantum Electronics, Snowbird, Utah, Jan. 2-6, 2006.
4. "The Quantum Information Revolution: Einstein's Legacy", Valparaiso University Physics Dept. colloquium, Feb. 24, 2006.
5. "Relativistic Quantum Cryptography", Evan Jeffrey and Paul Kwiat, APS March Meeting, Mar. 13-17, Baltimore, MD (2006)
6. "Optical resources for quantum information processing", Workshop on Linear Optical Quantum Information Processing (LoQUIP), Lousiana State University, Baton Rouge, Louisiana, April 10-12, 2006.
7. "Hyperentanglement: Generation and Applications", Julio Barreiro, Nicholas Peters, Nathan Langford and Paul Kwiat, CLEO/QELS 2006, May 21-26, Longbeach, CA (2006)
8. "The Quantum Information Revolution: 101 Uses for a Schroedinger Cat", Distinguished Lecture, Oak Ridge National Laboratory, July 11, 2006.
9. "Relativistic Quantum Cryptography", Paul Kwiat, Conference on Quantum Information and Quantum Control II, Univ. of Toronto, Canada, Aug. 8-11, 2006.
10. "Hyperentanglement for Quantum Communication: Remote Preparation of Single-photon Entangled States", Julio T. Barreiro, Nicholas A. Peters and Paul G. Kwiat, International Conference on Quantum Foundation and Technology: Frontier and Future (ICQFT06), Zhejiang University, Hangzhou, China (Aug. 26-29, 2006)
11. "Relativistic Quantum Cryptography", Evan Jeffrey and Paul Kwiat, APS March Meeting, Baltimore, MD (Mar. 13-17, 2006)

Number of Presentations: 11.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

"Remote State Preparation: Arbitrary remote control of photon polarizations for quantum communication", N. A. Peters, J. T. Barreiro, M. E. Goggin, T.-C. Wei, and P. G. Kwiat, Proc. SPIE, Quantum Communications and Quantum Imaging Conference III (Aug. 2-6, 2005), Ronald Meyers, ed.

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 1

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

(d) Manuscripts

"Relativistic Quantum Cryptography", Evan Jeffrey, Joseph Altepeter, and Paul Kwiat, in preparation
"High-speed Quantum Random Number Generation", Evan Jeffrey, Gleb Akselrod, Joseph Altepeter, and Paul Kwiat, in preparation
"Remote Entangled-State Preparation", Julio Barreiro and Paul Kwiat, in preparation

Number of Manuscripts: 3.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED	
Evan Jeffrey	0.50	No
Joe Altepeter	0.50	No
Julio Barreiro	1.00	No
Joseph Yasi	0.25	No
Michael Wayne	0.25	No
FTE Equivalent:	**2.50**	
Total Number:	**5**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED	
Joe Altepeter	0.25	No
FTE Equivalent:	**0.25**	
Total Number:	**1**	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Paul Kwiat	0.08	No
FTE Equivalent:	**0.08**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	
Philip Makotyn	0.25	No
Rachel Hillmer	0.25	No
Kevin Uskali	0.25	No
Gleb Akselrod	0.10	No
FTE Equivalent:	**0.85**	
Total Number:	**4**	

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME		
Joe Altepeter	No	
Total Number:	**1**	

Names of other research staff

NAME	PERCENT_SUPPORTED	
Mike Goggin	0.06	No
FTE Equivalent:	**0.06**	
Total Number:	**1**	

Sub Contractors (DD882)

Inventions (DD882)

5 **Quantum Random Number Generator**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2): World

5a: Paul Kwiat

5f-1a: UIUC

5f-c:

5a: Evan Jeffrey

5f-1a: UIUC

5f-c:

5a: Joseph Altepeter

5f-1a: UIUC

5f-c:

Advanced Quantum Communication Protocols
45564PHQC
ARO/DTO: DAAD190310282

Abstract:

We have realized the first demonstration of "relativistic" quantum cryptography, using both faint laser pulses and entangled photons. By incorporating an optical delay cavity, Bob is able to measure every photon from Alice in the correct basis, leading to enhanced key rates, as well as some security advantages. We have also implemented our proposal for a high-speed quantum random number generator, in which the arrival time of a detected photon is used to generate ~8 random bits per photon. Our system produced cryptographically secure bits at over 4 Mbits/s, with a clear path toward even higher rates. In addition, we solved a number of technical problems to produce 99%-fidelity polarization-entangled pairs from a diode-laser pumped source. Extending our previous implementation of remote state preparation, we have incorporated hyperentanglement to successfully remotely prepare *entangled* states. Finally, we studied the use of hyperentangled photons as a resource for improved quantum dense coding. Although our experimental verification is still in progress, we identified the theoretically optimal configuration, and compared hyperentangled and multi-pair encoding.

Table of Contents:

Figures:

Advanced Quantum Communication Protocols: Summary of Main Results

- 4- and 6-state "relativistic" quantum cryptography realized with faint laser pulses and entangled photons: 2-4% BERs, yield enhancement = 1.3 (4-state), 2.1 (6-state)
- Proof-of-principle time-bin based quantum random number generator implemented, generating ~8 bits/photon (at 720 kHz) 4.3 MHz final random bit rate
- High-quality (F = 99%, T = 97%) polarization entanglement realized with laser diode-pumped BiBO source (for 405 → 810 + 810 nm)
- Diode laser-pumped nondegenerate (405 → 772 + 852 nm) entanglement produced
- Hyperentanglement used in remote-state preparation of various entangled states with F > 90%, T > 87%
- Limits found on hyperentanglement-based quantum dense coding with linear optics and projective measurements; experimental configuration to achieve limit found.
- Experimental realization of 4-state quantum dense coding in progress (using improved holograms in novel polarization/spatial-mode interferometer)

Some previous results:

- Implemented first "quantum orienteering" protocol, demonstrating that 2 anti-parallel spins encode information more faithfully than 2 parallel spins
- Implemented first remote-state preparation protocol, generating pure and mixed states (both degenerate and non-degenerate), with average fidelity > 99%
- Proposed new method for fast quantum random number generation, using photon arrival time to obtain multiple random bits per photon.

Advanced Quantum Communication Protocols:
Scientific Progress and Accomplishments

"Relativistic" Quantum Cryptography

We have implemented relativistic quantum cryptography (RQC) using both an attenuated classical source and polarization-entangled photons, allowing increased communication efficiency over the usual BB84 protocol. To do so, it requires Bob to store photons received from Alice until *after* the classical communication phase, thereby allowing him to measure each photon in the correct basis, eliminating the loss from the sifting step of BB84. Greater advantages are possible in the six-state protocol, which uses an additional basis to improve sensitivity to eavesdropping but normally suffers greater sifting loss of 67% instead of 50%. However, there is a price for the enhanced bit rate afforded by RQC: Alice and Bob must ensure that they have synchronized clocks in order to prevent Eve from obtaining the basis information before Bob has received and stored his signal. This allows Alice and Bob to be certain that the backward light cone of when Bob received the photon and the forward light cone of when Alice sent the classical basis information do not overlap. Under this relativistic constraint, there is no frame of reference in which an eavesdropper could have access to both the quantum and the classical signal, and the usual quantum cryptography security proofs apply.

In our implementation, we used an adjustable optical delay line constructed from cylindrical mirrors, allowing delays from 13 ns to several microseconds. The delay required depends on the latency of the classical communication. Most high speed networking protocols have latencies much higher than the maximum available storage time, so in order to meet the requirements for the RQC protocol, we implemented an optical communication system based on high-speed programmable logic to achieve a total end-to-end latency of 160 ns, and used a 484-ns optical delay with a 67% storage efficiency[1].

We initially implemented the RQC protocol using attenuated laser diodes (see Fig. 1a). One often overlooked risk of such faint-pulse cryptography is that the 4 (or 6) states may not be indistinguishable. For instance, in our system we used 4 different laser diodes, each polarized differently. However, unless the properties of the diode lasers are carefully matched, they will in general have different pulse shapes and frequencies. Any non-identically of the pulses can potentially leak information to the eavesdropper who can – in principle – measure that property without disrupting the polarization. Similar difficulties can also exist in phase-shift based systems. Therefore, we spent no small amount of effort in making the output pulses temporally very similar (see Fig. 1b); additionally, a 1-nm bandwidth interference filter was used to enhance the *spectral* similarity, although no detailed tests were made to quantify this (such tests are in fact rather difficult, and one reason that entangled photons offer such an advantage over faint-pulse cryptography).

[1] We have measured the reflectivity of our mirrors to be 99.80%, substantially less than the specified 99.95%. It is possible that cleaning these mirrors will restore the higher reflectivity. If so, then our storage cavity should attain a net transmission of ~90%.

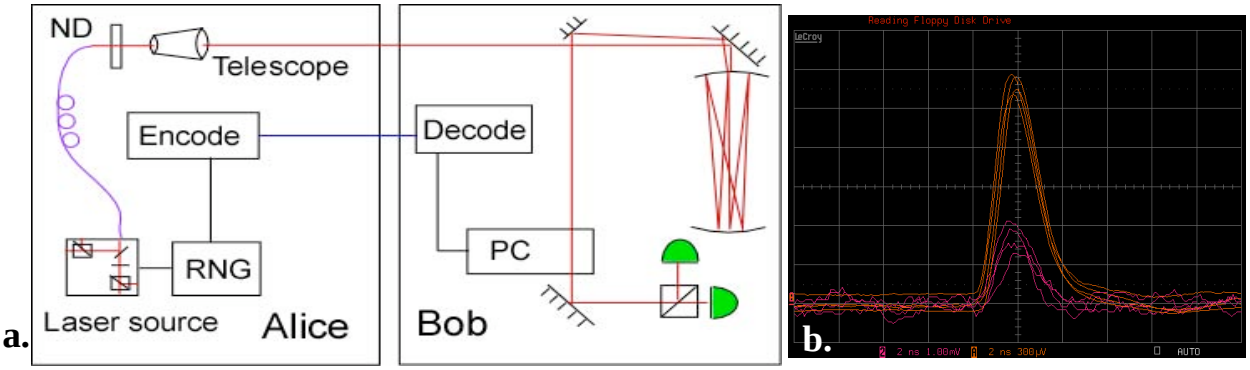


Fig. 1 a) Setup for implementing attenuated-laser relativistic QKD. b) Overlapping traces of pulses from four optimized diode lasers, one for each polarization state.

Using a 10-kHz repetition rate and a mean photon numbers of 0.1, 0.5, 0.7, and 1 photon per pulse, we achieved 840 secret bits/s, an improvement of 12% over the 750 bits/s with standard BB84 (i.e., when the cavity was not used). This advantage is below the near-100% theoretical maximum, mostly due to the 33% loss in the storage cavity (the upper limit to the enhancement factor for the BB84 protocol is 2T □1, where T is the net transmission of the cavity), and also due to a slight increase in bit error rate with the cavity in place. Improved cavity efficiency would allow us to raise this significantly. In addition, it could potentially improve efficiency further when coupled with the six-state protocol.

We also implemented RQC with an entangled photon source (Fig. 2a), thereby completely avoiding the issue of unmatched laser diodes and the associated potential security loophole alluded to above. In particular, with entangled photons it is easy to test for distinguishing information: any distinguishability between the photon pairs will act as decoherence, contributing to the measured error rate just as if an eavesdropper had access to those degrees of freedom. The use of entangled photons has a further advantage over faint-pulse systems, in that the former are not as susceptible to photon number-splitting attacks, which limit the range of faint-pulse systems.

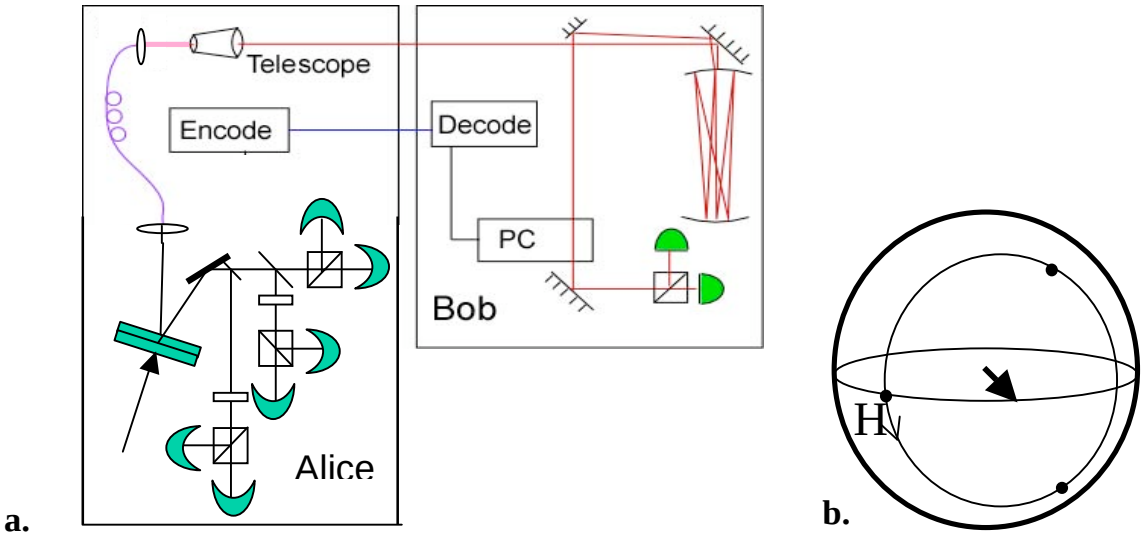


Fig. 2 a. Setup to implement 6-state RQC with entangled photons. b. Poincare sphere showing the basic concept to realize polarization analysis in 3 mutually unbiased bases, by applying voltages of 0, ±V to a single Pockel cell (induced optics axis indicated by the arrow).

Using our previously demonstrated source of non-degenerate polarization entanglement (351 nm → 670 nm + 737 nm), we implemented relativistic versions of both BB84 and the six-state protocol. In the latter case we introduced a novel analysis technique, whereby a set of 3 bases can be accessed via a *single* Pockel cell (PC). With no voltage applied, the input polarization is unchanged, and analysis proceeds in the H/V basis; applying a voltage of $\pm V$ causes H polarization to rotate to either of the two other mutually unbiased bases (points indicated in Fig. 2b).

We were able to show a 1.3 improvement above the expected rate without delayed choice for BB84, and a factor of 2.1 increase for the six-state protocol (where the theoretical maximum enhancement factor is 3); a comparison of the yields for various error rates is shown in Fig. 3. Due to the limited brightness of our source, the final key rates were substantially lower (~100-250/second). However, while our implementation functions at a relatively low overall bit rate, these techniques could be directly applied to systems running at higher speeds (one of the main limitations being the rate of Pockel cell switching).

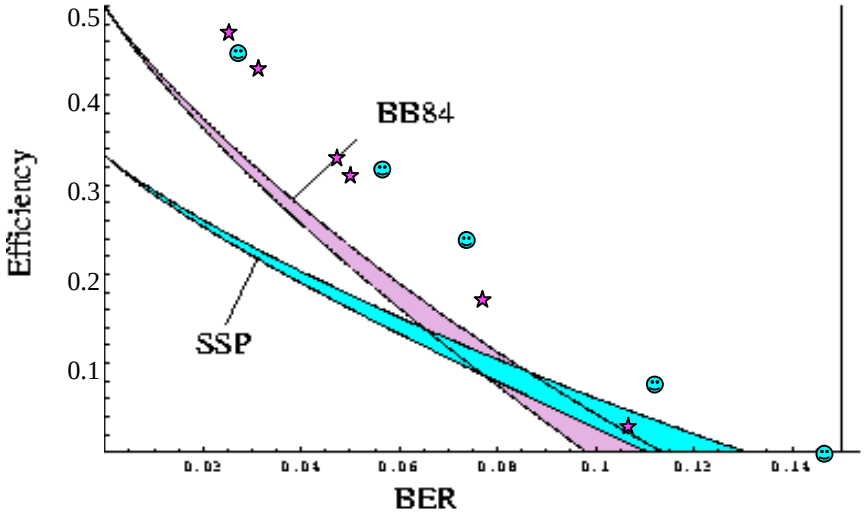


Fig. 3 Plot showing the usual efficiency (after error detection and privacy amplification) of the 4-state (BB84) and 6-state (SSP) protocols, in addition to the efficiencies we achieved (data points) in our delayed-choice implementation.

Our results show a definite improvement in key exchange rate for the relativistic protocols, one of only a few instances known where adding relativistic constraints can improve over purely quantum protocols. One initial conclusion might be that the added complexity of the protocol (including cavity alignment, stability, loss, slight polarization transformation, and the necessity of synchronized clocks) outweighs the modest gains in final secret key rate. However, there may be other reasons to prefer RQC. Specifically, the delayed-choice protocol avoids some potential attacks present in standard quantum key distribution, where reconciliation is performed well after key exchange[2]. For instance, some attacks rely on disrupting the classical communication phase to force Alice and Bob to "forget" that they had a basis agreement for the bits where Eve created errors. If she does this, Eve can hide her influence in the bits thrown out while sifting. In RQC, Alice and Bob use the same basis every (or nearly every) time, making this sort of attack ineffective.

[2] We are grateful for helpful discussions on these points with Dr. Dude "Michael" Neergaard (ORNL).

Quantum Random Number Generator

As discussed in the patent section of our August 2005 annual report, we have proposed a novel idea for a quantum random number generator (QRNG), based on the arrival times of single photons at a detector[3]. One established method to generate quantum mechanically random numbers is to simply record which way a single photon goes at a 50-50 beamsplitter. The operating rate of such scheme is limited by the deadtime of the detectors to ~1 MHz. Our new approach is to use the *time* of the detection event as the random variable. Because this can be measured to a much smaller interval than the detector dead time, it is possible to obtain over 10 random bits per photon detection.

Three configurations of the QRNG were first numerically simulated. In the first configuration, the light source intensity is kept constant, and the time-interval analyzer (TIA) is reset only after a photon was detected. In the second configuration, the intensity is also kept constant, but the TIA is reset either by a periodic trigger or by the detection of a photon, whichever occurred first. The first two configurations produce an exponentially decaying time-interval probability distribution, and thus a nonuniform distribution of random numbers. To correct this a whitening algorithm must be applied to these data (see below). In order to avoid or reduce the computational task of whitening, a third configuration was investigated, in which the intensity is ramped periodically (see Fig. 4), leading to a flat time-interval probability distribution. Each of the three configurations was simulated for various time resolutions, assuming a detector with a 50-ns dead time. The results show that the entropy rate (random bits per second) is ~7% lower when using the third configuration compared to the other two; thus, while ramping the light intensity is a viable method to reduce whitening, it does not have an intrinsic advantage in terms of the final rate of random bits.

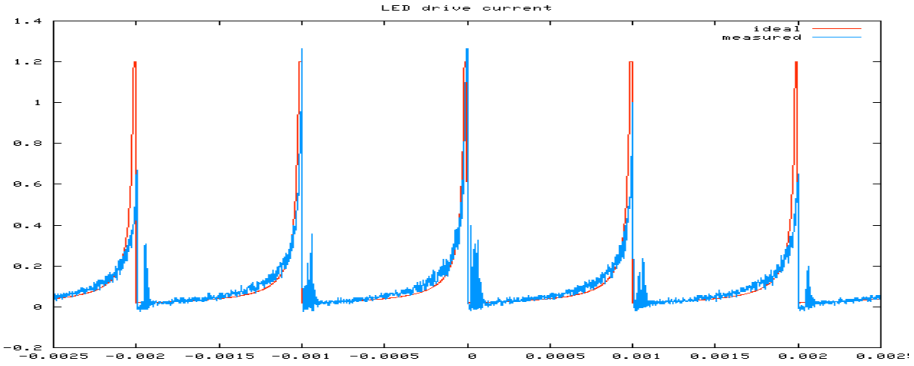


Fig. 4 Intensity ramp (red, theory) to generate a near-constant time-interval probability distribution; in blue is the output of a custom LED-drive circuit.

We have thus far implemented the first QRNG scheme, with a constant intensity light source (Fig. 5). Arrival times between successive photon-detection events are intrinsically unpredictable, and are measured to generate a high-rate source of entropy. The arrival

[3] The patent application on our Quantum Random Number Generator was extended to a worldwide application. In the process, it was discovered that this concept was, in fact, patented several years ago by Lo, Lutkenhaus, et al. To our knowledge they did not reduce this concept to practice as we have, but we have nevertheless been advised to withdraw our patent.

times are seen to be exponentially distributed (the expected waiting time for a Poisson process). Most applications require not only a high rate of total entropy produced, but also high entropy *density*, i.e., each outcome is nearly equally likely. To this end, we implemented a "compression", or "whitening" algorithm to take the low-density random numbers from our measurement of arrival times and convert them to a smaller number of high density random bits. This was achieved by using a hash function (SHA-1) with a fixed size output buffer (160 bits), and feeding it enough raw entropy that all 2^{160} possible outcomes are very close to equally likely.

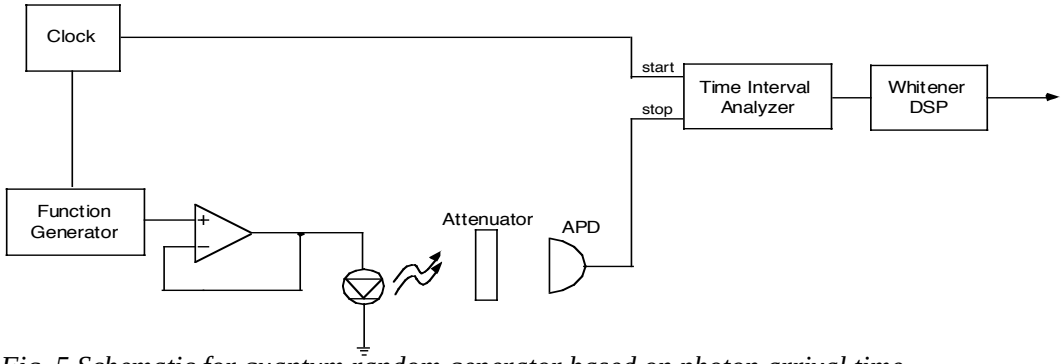


Fig. 5 Schematic for quantum random generator based on photon arrival time.

In our present implementation, the light source is an attenuated LED (constant intensity), the timing information is measured with a National Instruments NI-6602 timer board (with 12.5-ns resolution), and the single-photon detector was an avalanche photodiode (APD), counting at rates up to ~720 kHz.[4] We experimentally measure the average entropy to be 8 bits/detection event, showing the clear advantage of deriving randomness from photon arrival time, compared to generators that measure which way a photon travels at a beam splitter (and hence only generate at most 1 bit/photon). Some of this total entropy is lost in the hashing process to allow for collisions in the hash function (present in all such compression functions). Our final rate of random number generation after whitening is 4.3 Mbit/s, corresponding to 7.34 bits/detection event. The generated random numbers pass all FIPS tests, and we calculate the Shannon entropy of the output to be > 0.99999/bit; thus, almost all bias and predictability is removed (a theoretically "perfect" random number generator would produce 1 bit of entropy for every output bit). The "min entropy" for an entire 160-bit block from the hash function is greater than 159.5 bits, representing how unlikely it is for an adversary to guess an entire block on the first try. This is then a measure of the worst-case performance of our random number generator.

This speed of quantum random number generation is already comparable to the fastest available true random number generators. However, with the implementation of custom electronics, rather than computer and Labview-based data acquisition, the system could be made substantially faster. APDs are capable of detecting photons at up to several MHz, which should allow generation of random numbers exceeding 10 Mbit/s, while much faster rates may be achievable by using high speed photomultiplier tubes (PMTs), which can have maximum count rates much higher than APDs.

[4] These detectors can run about five times faster, which in principle would lead to higher random bit rates (not five times faster though, since the shorter interval between detection events implies fewer available time-bins in which a photon could be detected); however, our present timing board precludes faster operation.

Portable Entanglement Source

As discussed in past annual reports and reviews, we've been attempting to drive our 2-crystal spontaneous parametric downconversion (SPDC) entanglement source using a diode-laser pump (at 405 nm). We had previously observed reduced entanglement from such a source, and developed a preliminary theoretical model to explain this phenomenon. There are two factors that limit the degree of entanglement achievable with a diode pump laser: the relatively short coherence length of the light and the fact a free-running diode laser can support several longitudinal modes. One consequence is that the down-conversion photons associated with slightly different pump wavelengths are emitted in slightly different directions – propagation through the birefringent down-conversion crystals then leads to different phase shifts, which show up as decoherence. To address this, we implemented a frequency-stabilized pump diode laser, which partially improved the problem. Related to this, we acquired a custom volume holographic grating, which should allow us to achieve frequency stabilization of our diode laser with higher efficiency, and a much smaller footprint (important if one is moving toward robust, compact, practical sources). We have spent some time trying to characterize the new grating, and unfortunately the preliminary conclusion seems to be that it reflects back about ten times less light than it was specified for. Further tests are still underway.

Meanwhile, however, in the last year we discovered an additional effect that leads to reduced entanglement in the diode-pumped sources, namely, temporal walkoff of the polarization components of the pump, leading to effective decoherence. We found that a temporal precompensation scheme (adding a particular birefringent crystal into the pump beam before the downconversion crystals) substantially improves the tangle of cw diode sources utilizing the two-crystal SPDC scheme. Using this precompensation technique, we extended our previous single-crystal measurements of downconversion in BiBO to generate high quality polarization entanglement with a diode laser pump (405 → 810 +810 nm) achieving 99% fidelity and 97% tangle (similar results were also obtained with an argon-ion laser pump: 351 → 702 + 702 nm). From the measured density matrix (Fig. 6), we can

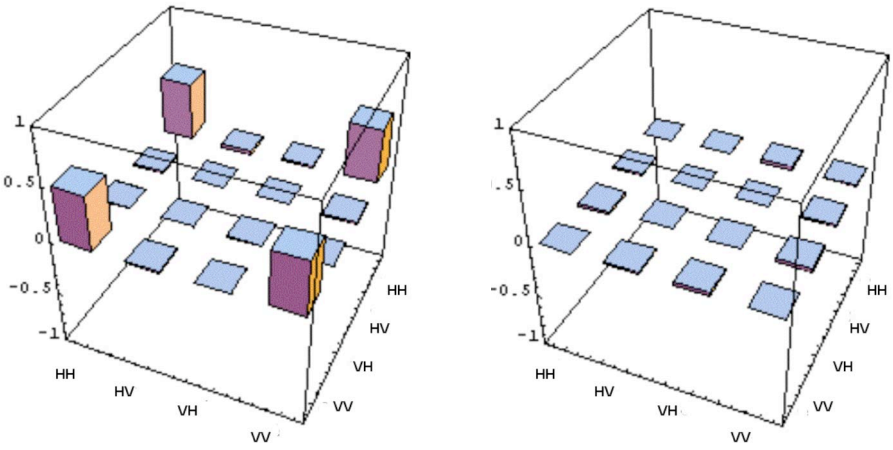


Fig. 6 Real (right) and imaginary parts of the measured density matrix for polarization-entangled state created using diode-laser pumped BiBO crystals. This state had 99% fidelity with a maximally entangled state, and tangle 0.97.

estimate the implied bit error rate if such a source were to be used in a quantum cryptography setting; we find <BER> = 0.8% (where the average is over the horizontal/vertical, diagonal, and circular bases). We are now attempting to duplicate these results with a nondegenerate diode-pumped source, running 405 → 772 + 852 nm, as 772 nm is nearly optimal for free-space atmospheric transmission. Our preliminary results are somewhat encouraging (92%-visibility, implying a tangle >90%), but further investigation is needed.

Remote Entangled-State Preparation

Previously as part of this project we investigated the novel quantum communication protocol of remote state preparation, whereby, by using an entangled pair of particles, Alice is able to precisely control Bob's qubit, conditional on the outcome of measurement results on her side. This is rather like quantum teleportation, except in this case Alice knows the state she is trying to transmit to Bob. Consequently, this protocol is substantially easier to implement than quantum teleportation (no Bell-state analysis is required, and only a single bit of classical information needs to be sent to Bob), although the average efficiency is limited to ~50%. As we reported last year, using polarization-entangled photon pairs generated via spontaneous parametric downconversion, we were able to realize this protocol to remotely prepare a wide variety of states, both pure and mixed, with extremely high fidelities (average greater than 99.5%).

As part of a separate project (MURI with Stanford), we previously implemented a high-quality source of photon pairs that were simultaneously entangled – "hyperentangled" – in every degree of freedom: polarization, orbital angular momentum (OAM), and time-energy. We verified entanglement by quantum state tomography, and observed a Bell-type inequality violation in each degree of freedom; we produced maximally hyperentangled states, with tangles of over 0.96 in each degree of freedom. Using this source, and a more generalized set of projectors on Alice's side (e.g., projectors that couple measurements of polarization and spatial mode) Alice can remotely prepare 2-qubit single-photon states on Bob's side, including *entangled* states. Such a capability could be an element of a larger quantum communication protocol.

Specifically, if Alice and Bob each have one member of a hyperentangled pair in the state

$$(|H_{rp}H_t\rangle + |V_{rp}V_t\rangle) \otimes (|l_{rp}r_t\rangle + |r_{rp}l_t\rangle)$$

and Alice makes a projection onto the state

$$\cos\theta\,{}_t\langle Hr| + e^{-i\phi}\sin\theta\,{}_t\langle Vl|$$

then, conditional on her detecting this photon, Bob's photon will be remotely prepared in the following state:

$$\cos\theta|Hl\rangle_{rp} + e^{i\phi}\sin\theta|Vr\rangle_{rp}$$

To perform the projective measurement in the two-degree of freedom Hilbert space, we have implemented a novel polarization/angular-momentum interferometer (see Fig.7a). The first beam splitter of the interferometer consists of a hologram, which directs the +1 and –1 orbital angular momentum states (after converting them into Gaussian modes) into different directions. These are then combined on a polarizing beam splitter (PBS).

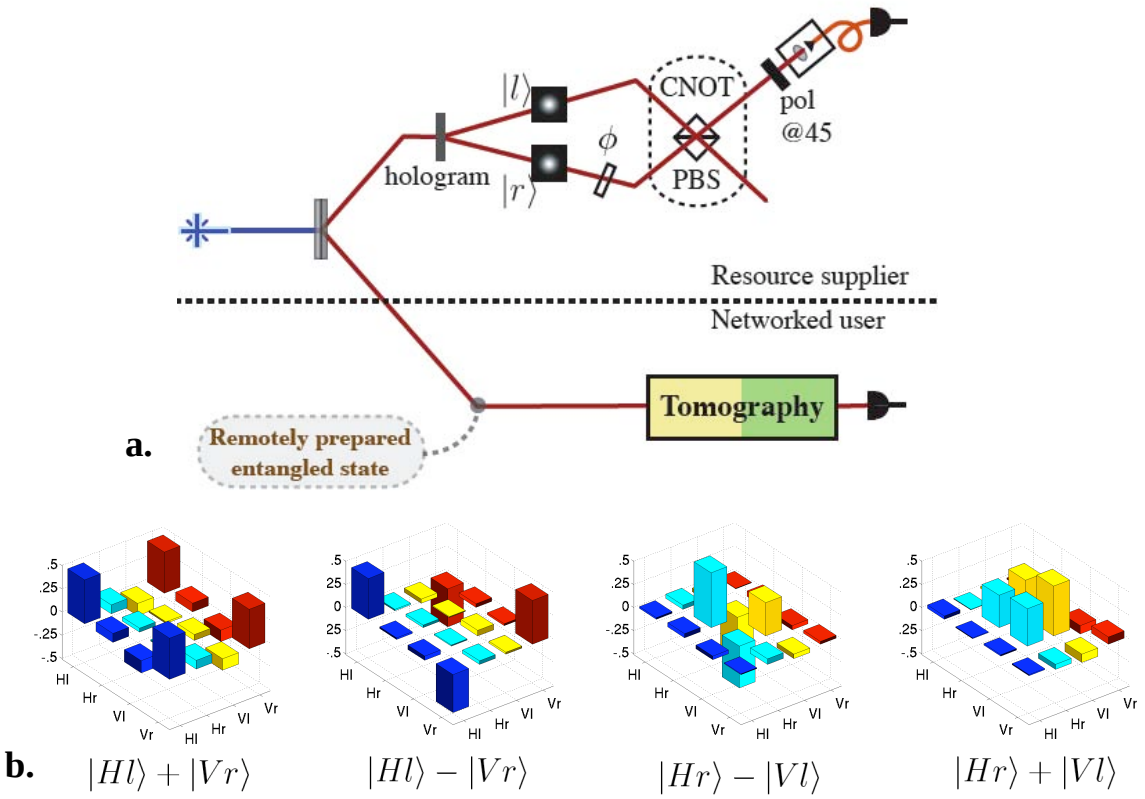


Fig. 7 a. Setup to implement remote entangled-state preparation. The novel interferometer projects the Resource Supplier's photon onto an entangled state of the polarization and spatial-mode degrees of freedom of her photon. The hyperentangled nature of the photon pair ensures that the receiver Bob's photon is then projected onto a similar single-photon entangled state. b. Experimental tomographies (real part) of four canonical polarization/spatial-mode entangled Bell states.

Detecting a photon in one output after a polarizer at 45˚ projects Alice's target photon into the state listed above. With this scheme we have successfully remotely prepared a variety of entangled states (Fig. 7b), with average fidelity of ~90%, and ~85% tangle between the spatial-mode and polarization degrees of freedom.

Quantum Dense Coding

Due to the limitations of linear optics quantum information processing, it was initially believed impossible to completely and efficiently distinguish all four polarization Bell states with a single measurement. Only two out of the four Bell states could be unambiguously distinguished, although one could choose a set of three Bell states such that any state within the set can be distinguished from the other two. However, several years ago Harald Weinfurter and I showed that indeed it is possible to distinguish all four Bell states, if the photons were simultaneously entangled in more than one degree of freedom. Our hyperentangled photon source provides precisely the needed correlations. Once one can reliably distinguish all four Bell states with a single measurement, one can incorporate this capability into an optimized quantum dense-coding protocol. The simplest setup to realize this, not requiring any two-photon interference, is shown in Fig. 8.

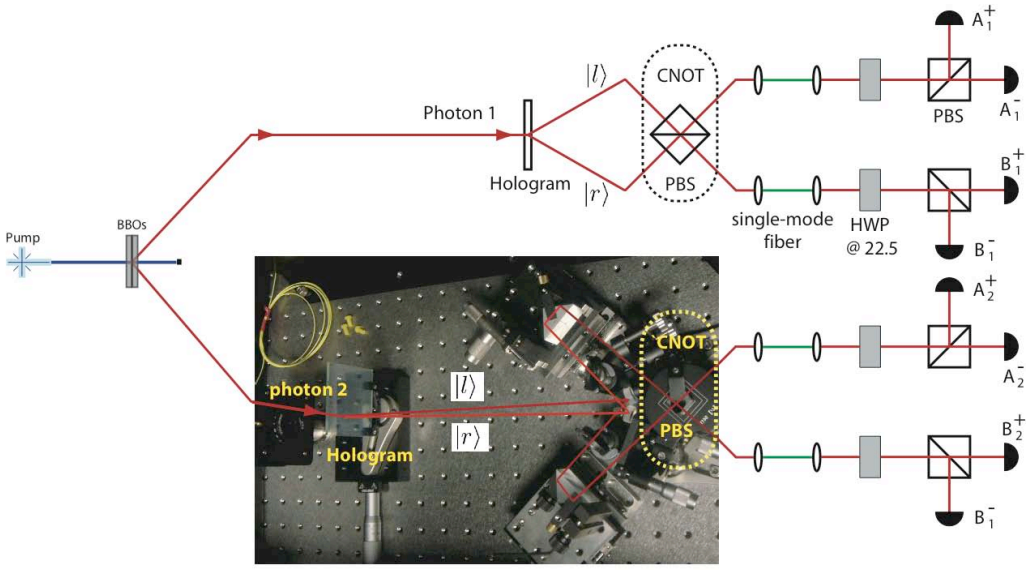


Fig. 8 Setup to implement full polarization Bell-state analysis, using hyperentangled photons.

For example, if the photons are prepared in the state $\begin{pmatrix}\Phi^{\pm}\\ \Psi^{\pm}\end{pmatrix}\otimes\phi^{+}$

where the first state is one of the four polarization Bell states, and the second is a spatial-mode Bell state, then the following detector coincidence signatures will hold:

State	Detector signature			
$\|\Phi^{\pm}\rangle$	$A_1^+A_2^{\pm}$	$B_1^+B_2^{\pm}$	$A_1^-A_2^{\mp}$	$B_1^-B_2^{\mp}$
$\|\Psi^{\pm}\rangle$	$A_1^+B_2^{\pm}$	$B_1^+A_2^{\pm}$	$A_1^-B_2^{\mp}$	$B_1^-A_2^{\mp}$

We have previously shown that we can readily produce all four of the polarization-entangled Bell states, with very high fidelity. The implementation of quantum dense coding is then straightforward: One photon of each hyperentangled pair is sent to Alice and Bob. Using waveplates on her photon alone, Alice can modify the joint polarization Bell state; she then sends her photon to Bob, who can make a joint measurement (Bell state analysis) on the two photons, to determine which of the four polarization Bell states Alice generated.

As part of our MURI grant with Stanford, we have been attempting to implement hyperentanglement-enabled full Bell state analysis. We have successfully constructed the necessary polarization/spatial-mode interferometers, achieving 98% visibility, stable over an hour. However, we discovered that our holograms had an extinction ratio (the ability of the hologram to filter out all unwanted states) of only ~10:1. Recently we created new holograms and improved our mode-coupling technique, resulting in improved extinction up to 1000:1. We are currently in the process of incorporating the new holograms into our interferometers; once this system is aligned, we can then readily demonstrate both Bell state analysis and quantum dense coding, the final milestone of this grant.

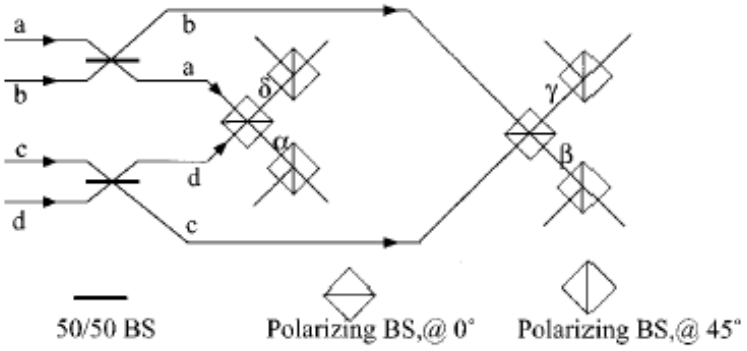
In fact, if two photons are in a hyperentangled state with entangled polarizations and momenta (and assuming there are two momentum – or two orbital-angular-momentum – states associated with each photon), then there are 16 Bell-like states in total. As discussed above, it is relatively easy to distinguish, e.g., all four polarization Bell states, in a single

measurement. The question naturally arises, given a particular hyperentangled state, what is the maximum number of generalized Bell states (i.e., including entanglements across degrees of freedom) which may be reliably distinguished using a suitable projective measurement that is limited to linear optics techniques. One of our goals was to identify this theoretical upper limit for dense coding using a hyperentangled resource, and to devise a practical method for achieving it.

We have now shown that, in fact, *none* of the 16 states can be uniquely identified. Instead, the optimal state-discrimination is such that the 16 states are divided into 7 groups, where states from different groups can be distinguished. One consequence of this result is that we can choose 7 states to perform superdense coding, which would give $\log_2(7) \sim 2.8$ classical bits. We have proved that this is the optimal, given strong projective measurements, verifying that only 7 groups may distinguished in each of the 16!/8!/8! = 12870 cases. We are currently exploring the effect of generalized measurements (POVMs) and the implications for quantum teleportation and fingerprinting.

Fig. 9 shows one experimental implementation that should achieve this optimal situation of 7 resolvable groups, and the predicted experimental signatures for each one. The subsequent table summarizes the number of distinguishable states, depending on whether one or two pairs are used, and on whether a single or two degrees of freedom are used. We can draw several conclusions:

- Due to the limitations of linear optics analysis, in no case can one use an "unbiased" encoding, i.e., there are always states that give the same experimental signature. Therefore, for super-dense coding Alice should use a "biased" encoding, where she limits herself to distinguishable *groups*, instead of states.
- Strictly in terms of the maximum number of resolvable groups, the optimal situation is to use two pairs of photons, each entangled in only a single degree of freedom; 9 groups may then be distinguished.
- However, unless one has access to photon-number resolving detectors, one cannot distinguish all 9, but only 4. In this case, one is better off using a single hyperentangled pair, for which 6 states can be reliably distinguished.
- In practice, a single hyperentangled pair is always like to be (much) more efficient than two singly entangled pairs, for the reason that the latter require 4 photons to be detected (with a net efficiency that varies as η^4), whereas only 2 photons need be detected in the hyperentangled pair case (with a net efficiency that varies as η^2). As long as the detector efficiency is less than $\sqrt{7/9} = 88\%$ (82% if the detectors cannot resolve photon number), the hyperentangled superdense coding is most efficient.



State	Detector signature
$\Phi^+ \otimes \phi^+$, $\Phi^- \otimes \phi^-$, $\Psi^+ \otimes \psi^-$, $\Psi^- \otimes \psi^+$	$\alpha_{45}\alpha_{45}$, $\alpha_{\overline{45}}\alpha_{\overline{45}}$, $\beta_{45}\beta_{45}$, $\beta_{\overline{45}}\beta_{\overline{45}}$, $\delta_{45}\delta_{45}$, $\delta_{\overline{45}}\delta_{\overline{45}}$, $\gamma_{45}\gamma_{45}$, $\gamma_{\overline{45}}\gamma_{\overline{45}}$
$\Phi^- \otimes \phi^+$, $\Phi^+ \otimes \phi^-$	$\alpha_{45}\alpha_{\overline{45}}$, $\beta_{45}\beta_{\overline{45}}$, $\delta_{45}\delta_{\overline{45}}$, $\gamma_{45}\gamma_{\overline{45}}$
$\Psi^+ \otimes \phi^+$, $\Phi^+ \otimes \psi^-$	$\alpha_{45}\delta_{45}$, $\alpha_{\overline{45}}\delta_{\overline{45}}$, $\beta_{45}\gamma_{45}$, $\beta_{\overline{45}}\gamma_{\overline{45}}$
$\Psi^- \otimes \phi^+$, $\Phi^+ \otimes \psi^+$	$\alpha_{45}\gamma_{45}$, $\alpha_{\overline{45}}\gamma_{\overline{45}}$, $\beta_{45}\delta_{45}$, $\beta_{\overline{45}}\delta_{\overline{45}}$
$\Psi^+ \otimes \phi^-$, $\Phi^- \otimes \psi^-$	$\alpha_{45}\delta_{\overline{45}}$, $\alpha_{\overline{45}}\delta_{45}$, $\beta_{45}\gamma_{\overline{45}}$, $\beta_{\overline{45}}\gamma_{45}$
$\Psi^- \otimes \phi^-$, $\Phi^- \otimes \psi^+$	$\alpha_{45}\gamma_{\overline{45}}$, $\alpha_{\overline{45}}\gamma_{45}$, $\beta_{45}\delta_{\overline{45}}$, $\beta_{\overline{45}}\delta_{45}$
$\Psi^- \otimes \psi^-$, $\Psi^+ \otimes \psi^+$	$\alpha_{45}\beta_{45}$, $\alpha_{\overline{45}}\beta_{\overline{45}}$, $\delta_{45}\gamma_{45}$, $\delta_{\overline{45}}\gamma_{\overline{45}}$

Fig. 9 Experimental scheme to distinguish 7 of the 16 possible 2 2 2 2 hyperentangled Bell states. The table lists the predicted coincidence signatures for each of the 16 states.

	1 DOF (polarization H/V; spatial modes h/v; etc.)	1 DOF (polarization H/V; spatial modes h/v; etc.)	2 DOFs (H/V *and* h/v)
# of pairs Detector efficiency)	One (η^2)	Two (η^4)	One (η^2)
Unbiased uniform source	2/4	4/16	0/16
Biased source & photon-number-resolving detector	3/3	9/9	7/7
Biased source & NO photon-number-resolving detector	2/2	4/4	6/6